



DEPARTMENT OF THE NAVY

DIRECTOR, SPACE AND NAVAL WARFARE
INFORMATION TECHNOLOGY CENTER
2251 LAKESHORE DRIVE
NEW ORLEANS, LA 70145-0001

CH-1 of 20 Jul 2001
Incorporated 20 Jul 2001

SPAWARINFOTECHCENINST 5530.1 CH-1
ITC201
20 Jul 2001

SPAWARINFOTECHCEN INSTRUCTION 5530.1

Subj: PHYSICAL SECURITY PROGRAM

Ref: (a) OPNAVINST 5530.14C
(b) DOD 5200.2-R
(c) DOD Directive 5200.28
(d) NAVRESINFOSYSOFFINST 11320.1
(e) SPAWARINFOTECHCEN ltr 5500 Ser ITC201/374 of 25 Jun 01

1. Purpose. To publish guidance and procedures for the Physical Security Program within the Space and Naval Warfare Information Technology Center (SPAWARINFOTECHCEN) per references (a) through (d). The Physical Security Program is a part of the total Security Plan at SPAWARINFOTECHCEN and addresses the protection of personnel and property.

2. Cancellation. NAVRESINFOSYSOFFINST 5530.1

3. Responsibility

a. The Director has the overall responsibility for the Physical Security Program.

b. The Security Manager is the principal advisor to the Director and is responsible for the management of the Physical Security Program.

c. The Physical Security Officer reports to the Security Manager and is responsible for the day to day operation of the Physical Security Program at SPAWARINFOTECHCEN.

4. Firearms. The SPAWARINFOTECHCEN Security Department must be ready to counter any threat to the facility. Due to the size of the command, value of its property, and degree of support provided by other security organizations, the Director may seek authorization from Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) for firearms to be issued to selected and auxiliary security personnel. Only those personnel named by the Director shall carry a firearm while at SPAWARINFOTECHCEN. (R)

5. Monitoring Service. Monitors perform multiple tasks to support the Physical Security Program of SPAWARINFOTECHCEN. Duties include:

- a. Monitoring personnel entering and exiting the facility.
- b. Monitoring SPAWARINFOTECHCEN Video Surveillance system.
- c. Monitoring alarm systems.
- d. Issuing access cards.
- e. Issuing visitor passes.
- f. Conducting building checks.

6. Command Zoning. SPAWARINFOTECHCEN will be zoned following the standards in reference (b).

a. SPAWARINFOTECHCEN zones are:

(1) Critical Sensitive Zone. (Single Scope Background Investigation (SSBI)).

(2) Non Critical Sensitive Zone. (National Agency Check with Inquiries (NACI)).

(3) Non Sensitive Zone. (NACI Investigation)

b. Employees entering a zoned area are required to have a security investigation completed at that level or higher.

c. The Physical Security Review Committee (PSRC) will determine the level for each zone.

7. PSRC

a. Per reference (a), members of the PSRC will be designated in writing and shall advise and assist in the implementation of SPAWARINFOTECHCEN zoning initiative and position category designation.

b. Members will include, but not be limited to:

(1) Security Manager

(2) Physical Security Officer

(3) Personnel Security Officer

(4) Information Security Manager

(5) Directorate directors or designees

(6) ACAT 1 Program Managers or Designees

c. Committee members or their representatives will meet quarterly. Minutes of the meeting will be made a matter of record.

8. Bomb Threats

a. Per reference (a), all threats will be presumed serious.

b. The following provides specific steps to take when threats are received by phone:

(1) Attract the attention of a nearby co-worker to advise that a threat is being received. Have them notify the Security Manager or Physical Security Officer. After working hours, notify the Dispatch Desk at extension 7-1500.

(2) Gather as much information as possible using the OPNAV 5327/8, Telephonic Threat Complaint.

(3) Ensure the Security Manager or Physical Security Officer has been notified.

(4) Personnel in the threatened area shall make a brief search of their immediate workspace for any unfamiliar boxes, bags, briefcases, etc.

(5) The Security Manager will notify the University of New Orleans (UNO) Police and initiate evacuation procedures.

(a) Employees will leave the building, following the fire drill procedures contained in reference (d).

(b) Employees should report any person(s) failing to leave or attempting to enter the building after evacuation to Security Office personnel.

(c) Employees will not reenter the building until authorized by the Security Office.

9. Access Control. Facility Access Cards will be issued to all employees of SPAWARINFOTECHCEN for command access purposes and will be worn so that they are visible at all times while on the complex.

a. Identifying Facility Access Cards. Access cards are designed in such a way as to readily identify government and contractor personnel and will be distinguishable as follows:

(1) Government - White Badge with:

- (a) Critical Sensitive - Red Stripe
- (b) Non Critical Sensitive - Blue Stripe
- (c) Non Sensitive - No Stripe

(2) Contractor - Blue Badge with:

- (a) Critical Sensitive - Red Stripe
- (b) Non Critical Sensitive - Blue Stripe
- (c) Non Sensitive - No Stripe

b. Civil Service and Military Facility Access Cards. The pictured facility access cards are issued to civil service and military employees working at this installation. These cards are not valid in excess of 4 years.

(1) Government employees must have a completed Facility Access Card Request form (SPAWARINFOTECHCEN 5512/1 (4-01)) signed by their directorate director or deputy providing the position category authorized. A picture Identification (ID) will be required to verify their identity.

(2) To renew the existing Facility Access Cards, the employee must submit an updated Facility Access Card Request form signed by their directorate director or deputy.

c. Contractor Facility Access Card Request. Issued to contract employees working at the SPAWARINFOTECHCEN and for contractors who have official business on this site.

(1) Initial facility access cards are issued upon receipt of the following:

(a) Notification of the contract award from the Contract Management Office (ITC00C).

(b) A Facility Access Card Request form (SPAWARINFOTECHCEN 5512/1) signed by the directorate director or deputy of the organizational area supported and the designated Contracting Officer Representative (COR).

(c) A picture ID to verify identity.

(2) To renew the existing Facility Access Cards, the employee must submit an updated Facility Access Card Request form signed by the designated COR.

d. Temporary Facility Access Card Requests (government and contractor)

(1) A temporary facility access card may be issued to a government or contract employee, but only after approval by their respective GS13 or above (for government) or the government project manager/deputy directorate (for contractor).

(2) Directorate director/deputy, ACAT 1 project manager/deputy, or direct report will be notified of all forgotten or lost badges. Replacement of lost or damaged facility access badges may require a fee.

e. Visitor Passes

(1) All visitors must report to the Security Office, show valid photo ID and state reason for visit. A point of contact or designated representative must be provided.

(2) The visitors point of contact:

(a) Must be associated with the reason for the visit.

(b) Will sign the visitor in and accept responsibility to monitor their presence while on site.

(3) Persons having business on consecutive days at SPAWARINFOTECHCEN must sign in at the Security Office each day to receive the current day's pass.

(4) Passes will be issued to children (except infants) for ID purposes. Children will not be allowed beyond the Security Office without adult supervision.

(5) A visitor having business at SPAWARINFOTECHCEN will be escorted at all times by a cleared employee.

10. Medical Incident. All SPAWARINFOTECHCEN personnel should respond to medical emergencies occurring within their purview.

- a. During regular working hours, call emergency services (dial 9 for dial tone then 911), and then call the Security Desk at extension 7-1500.
- b. After working hours, the Security Desk shall call emergency services and notify the chain of command.

11. Key Control Program. Reference (e) designates the Physical Security Officer as the Key Control Custodian. The Key Control Custodian will:

- a. Maintain SPAWARINFOTECHCEN's overall Key Control Program.
- b. Maintain a log showing keys on hand, keys issued, to whom keys were issued, date and time the keys are issued and returned, and the signatures of persons drawing or returning a key.

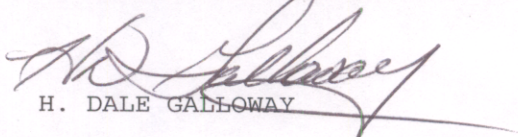
12. Administrative Inspection

- a. Hand carried items are subject to inspection prior to entering, while within, and upon departure of SPAWARINFOTECHCEN spaces.
- b. Inspections will be conducted as directed by the Director.
- c. Stairwells and elevators are considered outside of the command for the purpose of transferring classified material or government property.
- d. Authorized entry into any SPAWARINFOTECHCEN space constitutes consent to search personnel and property under their control.

13. Training. The Security Training Officer will ensure that security training is provided to all SPAWARINFOTECHCEN personnel as stated in reference (a).

14. Forms. The following forms mentioned within this instruction are stocked and maintained in the Security Office (SPAWARINFOTECHCEN (ITC201)).

- a. Telephonic Threat Complaint, OPNAV 5327/8.
- b. Facility Access Card Request, SPAWARINFOTECHCEN 5512/1 (4-01).


H. DALE GALLOWAY

Distribution: SPAWARINFOTECHCENINST 5218.1
Lists A, B, C, D, E, and F



DEPARTMENT OF THE NAVY

DIRECTOR, SPACE AND NAVAL WARFARE
INFORMATION TECHNOLOGY CENTER
2251 LAKESHORE DRIVE
NEW ORLEANS, LA 70145-0001

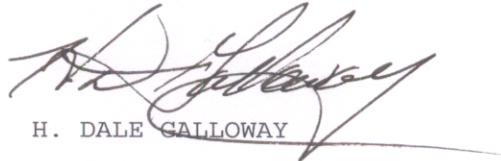
SPAWARINFOTECHCENINST 5530.1 CH-1
ITC201

SPAWARINFOTECHCEN INSTRUCTION 5530.1 CHANGE TRANSMITTAL 1

Subj: PHYSICAL SECURITY PROGRAM

Encl: (1) Revised Page 1

1. Purpose. To transmit change transmittal 1 to the basic instruction.
2. Action. Remove page 1 of the basic instruction and replace with enclosure (1) of this instruction.


H. DALE CALLOWAY

Distribution: (SPAWARINFOTECHCENINST 5218.1)
Lists A, B, C, D, E, and F